

**Congress of the United States**  
**Washington, DC 20515**

265

March 28, 2017

The Honorable Ajit Pai  
Chairman  
Federal Communications Commission  
455 12th Street, S.W.  
Washington, DC 20554

Dear Chairman Pai,

We are deeply concerned about the poor state of America's telecommunications cybersecurity. Our communications networks are far too vulnerable; the FCC has not, to date, prioritized cybersecurity; and the American people have largely been kept in the dark about the fact that their calls, texts, and movements are vulnerable to spying by foreign governments and hackers. This must change.

Cybersecurity researchers have issued repeated warnings about critical flaws in our communications infrastructure, including those in Signaling System 7 (SS7). However, cybersecurity has not traditionally been a regulatory priority for the FCC. Left, for the most part, to police itself, the cellular industry has neither adequately addressed these serious cybersecurity vulnerabilities nor warned its customers about the risks they face. Consequently, foreign governments and criminals can reach into U.S. cellular networks to track, surveil, and hack the phones of Americans.

The continued existence of these vulnerabilities—and the industry's lax approach to cybersecurity—does not just impact the liberty of Americans, it also poses a serious threat to our national and economic security. As such, the FCC must take swift action to address fundamental security threats to our mobile phones, which are no less dangerous than those cybersecurity threats that receive far more attention from other government agencies.

Last year, the FCC's Communications Security, Reliability and Interoperability Council (CSRIC) was tasked with looking into the SS7 cybersecurity issues that have been the subject of several media reports. On March 15, 2017, the CSRIC V working group 10 released a final report that includes a number of details that highlight the seriousness of this problem. In particular, the report:

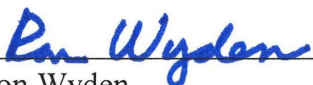
- Recognizes that wireline and 5G networks may be as vulnerable as cellular networks.
- Notes that "complicit or compromised operators means that all telecommunications protocols used to interconnect networks are potentially at risk."

- Identifies U.S. critical infrastructure that is vulnerable to cyber attacks.
- States that signaling aggregators will provide a wider view of signaling traffic and will reduce risk.
- Recommends a layered approach to security that includes “methods to protect the content of messages and voice communications by using end to end encryption.”
- Recommends improved firewalls to stop SS7 attacks.
- Notes that only a “handful of interconnection security experts in the world” focus on this issue.

Tasking the CSRIC with looking into this matter was a good first step, and the FCC should promptly implement the working group’s recommendations. However, CSRIC V’s charter ended on March 18, 2017, and, as the report notes, there are a number of related security issues that the group did not examine, as they were beyond the scope of the working group’s mandate. We urge you to establish a new CSRIC working group and to expand its scope to examine the remaining issues that were not previously explored by the CSRIC V working group 10.

It is clear that industry self-regulation isn’t working when it comes to telecommunications cybersecurity. We urge you to take swift action in this area in three ways. First, by forcing the cellular industry to address these serious cybersecurity vulnerabilities. Second, by warning the American public that their movements, communications, and devices may be vulnerable to foreign governments and hackers. And third, by promoting the use of end-to-end encryption apps, which, as the CSRIC working group stated, can be used to mitigate some of the SS7 risks.

Sincerely,

  
\_\_\_\_\_  
Ron Wyden  
United States Senator

  
\_\_\_\_\_  
Ted W. Lieu  
Member of Congress



FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON

OFFICE OF  
THE CHAIRMAN

June 15, 2017

The Honorable Ted Lieu  
U.S. House of Representatives  
236 Cannon House Office Building  
Washington, D.C. 20515

Dear Congressman Lieu:

Thank you for your letter concerning the security of America's communications infrastructure. I agree that we must have robust and resilient communications networks and that the Commission should foster such networks consistent with its statutory authority.

The Presidential Policy Directive on Critical Infrastructure Security and Resilience (PPD-21), released in 2013, reaffirmed a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure, including infrastructure in the communications sector. The Department of Homeland Security's Office of Cybersecurity and Communications serves as the sector-specific agency responsible for overseeing the preparedness of the communications sector with respect to cybersecurity.

The role that Congress and the President have prescribed for the FCC, in contrast, is a supporting one. We are to "partner" with the Department of Homeland Security and the Department of State on "(1) identifying and prioritizing communications infrastructure; (2) identifying communications sector vulnerabilities and working with industry and other stakeholders to address those vulnerabilities; and (3) working with stakeholders, including industry, and engaging foreign governments and international organizations to increase the security and resilience of critical infrastructure within the communications sector and facilitating the development and implementation of best practices promoting the security and resilience of critical communications infrastructure on which the Nation depends."<sup>1</sup>

Through the Communications Security, Reliability, and Interoperability Council (CSRIC), the Commission has done just that. Last year, the Commission tasked CSRIC V with seeking ways to address security vulnerabilities within the Signaling System 7 (SS7) protocol suite including authentication and encryption of SS7 network traffic.<sup>2</sup> As you mention in your letter, on March 15, 2017, CSRIC V issued several recommendations to mitigate SS7 vulnerabilities.<sup>3</sup> Among other recommendations, the report notes that security countermeasures—including signaling interconnection monitoring and filtering and subscriber encryption support—would help to reduce SS7 security risks. We have evaluated CSRIC V's recommendations and find that their implementation would improve the security and reliability of SS7 networks. Accordingly, we plan to encourage carriers to voluntarily implement CSRIC V's recommendations on SS7 risk mitigation strategies and to monitor their implementation. CSRIC V also recommended further work should be done by CSRIC on two emerging

---

<sup>1</sup> White House, Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil> (2013).

<sup>2</sup> See CSRIC Launches Group to Study Signaling System 7 Security, <https://blog.npstc.org/2016/06/28/csrlic-launches-group-to-study-signaling-system-7-security/> (2016).

<sup>3</sup> See WORKING GROUP 10 Legacy Systems Risk Reductions Final Report, <https://www.fcc.gov/files/csrlic5-wg10-finalreport031517pdf> (2017).



technologies: the Diameter protocol and 5G. We agree. Accordingly, we have tasked the next CSRIC, CSRIC VI, to recommend best practices to mitigate the network reliability and security risks associated with the Diameter protocol, an industry standard for connecting and authenticating subscribers on mobile networks. We have also tasked CSRIC VI to recommend mechanisms for designing and deploying 5G networks to mitigate risks to network reliability and security posed by the proliferation of Internet of Things devices and open-source software platforms used in 5G networks.

I appreciate your shared commitment to the security of our nation's communications infrastructure. I look forward to working with your office, as well as our partners at the Department of Homeland Security and the Department of State, to protect the communications sector from cyberthreats. Please let me know if I can be of any further assistance.

Sincerely,

A handwritten signature in blue ink, appearing to read "Ajit V. Pai".

Ajit V. Pai



FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON

OFFICE OF  
THE CHAIRMAN

June 15, 2017

The Honorable Ron Wyden  
United States Senate  
221 Dirksen Senate Office Building  
Washington, D.C. 20510

Dear Senator Wyden:

Thank you for your letter concerning the security of America's communications infrastructure. I agree that we must have robust and resilient communications networks and that the Commission should foster such networks consistent with its statutory authority.

The Presidential Policy Directive on Critical Infrastructure Security and Resilience (PPD-21), released in 2013, reaffirmed a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure, including infrastructure in the communications sector. The Department of Homeland Security's Office of Cybersecurity and Communications serves as the sector-specific agency responsible for overseeing the preparedness of the communications sector with respect to cybersecurity.

The role that Congress and the President have prescribed for the FCC, in contrast, is a supporting one. We are to "partner" with the Department of Homeland Security and the Department of State on "(1) identifying and prioritizing communications infrastructure; (2) identifying communications sector vulnerabilities and working with industry and other stakeholders to address those vulnerabilities; and (3) working with stakeholders, including industry, and engaging foreign governments and international organizations to increase the security and resilience of critical infrastructure within the communications sector and facilitating the development and implementation of best practices promoting the security and resilience of critical communications infrastructure on which the Nation depends."<sup>1</sup>

Through the Communications Security, Reliability, and Interoperability Council (CSRIC), the Commission has done just that. Last year, the Commission tasked CSRIC V with seeking ways to address security vulnerabilities within the Signaling System 7 (SS7) protocol suite including authentication and encryption of SS7 network traffic.<sup>2</sup> As you mention in your letter, on March 15, 2017, CSRIC V issued several recommendations to mitigate SS7 vulnerabilities.<sup>3</sup> Among other recommendations, the report notes that security countermeasures—including signaling interconnection monitoring and filtering and subscriber encryption support—would help to reduce SS7 security risks. We have evaluated CSRIC V's recommendations and find that their implementation would improve the security and reliability of SS7 networks. Accordingly, we plan to encourage carriers to voluntarily implement CSRIC V's recommendations on SS7 risk mitigation strategies and to monitor their implementation. CSRIC V also recommended further work should be done by CSRIC on two emerging

---

<sup>1</sup> White House, Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil> (2013).

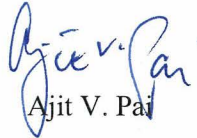
<sup>2</sup> See CSRIC Launches Group to Study Signaling System 7 Security, <https://blog.npstc.org/2016/06/28/csric-launches-group-to-study-signaling-system-7-security/> (2016).

<sup>3</sup> See WORKING GROUP 10 Legacy Systems Risk Reductions Final Report, <https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf> (2017).

technologies: the Diameter protocol and 5G. We agree. Accordingly, we have tasked the next CSRIC, CSRIC VI, to recommend best practices to mitigate the network reliability and security risks associated with the Diameter protocol, an industry standard for connecting and authenticating subscribers on mobile networks. We have also tasked CSRIC VI to recommend mechanisms for designing and deploying 5G networks to mitigate risks to network reliability and security posed by the proliferation of Internet of Things devices and open-source software platforms used in 5G networks.

I appreciate your shared commitment to the security of our nation's communications infrastructure. I look forward to working with your office, as well as our partners at the Department of Homeland Security and the Department of State, to protect the communications sector from cyberthreats. Please let me know if I can be of any further assistance.

Sincerely,



Ajit V. Pai